AWAITING CYBER 9/11

By CLIFFORD S. MAGEE

Enemies no longer need to launch missiles or fly airplanes into buildings to attack the United States. A new weapon has been introduced into the world's arsenal, and that weapon has no boundaries or rules, costs little, and has monstrous potential. The weapon is cyber warfare. The Nation's security, economy, and critical infrastructure are under cyber attack every day. Some attacks are from nation-states such as China and Russia, while others are from nonstate actors such as terrorist organizations, criminal gangs, teenage hackers, and anarchists. To protect American financial systems, power grids, telecommunications, water supplies, intellectual property, and military communications, the U.S. Government needs to designate the Department of Defense (DOD) as the lead organization in preventing, detecting, and recovering from cyber attacks.

In 2009, the *Wall Street Journal* reported that Chinese hackers had gained access to the U.S. electric power grid and created secret openings.[1] There was no monetary value in gaining control of the electrical grid, nor was there any intelligence value that would justify cyber espionage.[2] The only reason to penetrate the grid's controls was to prepare to combat American military superiority with asymmetrical cyberwar.[3] The Chinese had created a capability that could create power outages across the United States and possibly cause nuclear incidents without firing a shot. The victims were unaware their systems were compromised until the intrusions were detected by the U.S. Intelligence Community.[4] What would the U.S. Government have done if it discovered that China had been laying explosive charges throughout the national electrical grid system?[5]

The threats posed in the cyber domain are, in fact, an existential danger to the Nation. Currently, the United States does not have an organization with the capabilities or authorities to oversee cyber security for the public and private sectors. To develop this capability, the Nation needs to undergo a paradigm shift on how it views the cyber domain.

The Cyber Domain

In 1911, British naval theorist Julian Corbett in *Principles of Maritime Strategy* stated that the Royal Navy was necessary because it provided sea power to protect the goods and services that travel on the sea.[6] The British economy was based on trade, and the sea lanes for communications and trade were extraordinarily important for the security and prosperity of Britain. Today, the security and prosperity of the United States is dependent on cyber trade routes, but cyberspace is vulnerable to attack. Signals and information can be intercepted, interrupted, and exploited. The Nation must develop a strategy to defend the cyber domain similar to the strategies it developed for defending land, sea, and air domains.

Integrated DOD efforts defend these domains. Defending air trade and commercial routes is not the responsibility of the Federal Aviation Administration or American Air Lines; it is the responsibility of the Defense Department.[7] Similarly, Maersk Lines is not responsible for defense of the sea domain, but in the cyber domain, every American company is responsible for its own defense without support from the Government. The U.S. Government does not have a lead organization to defend all government networks from attacks, much less assist with defending the private sector. DOD needs to be assigned the responsibility of defending the cyber domain with assistance from the Department of Homeland Security, Intelligence Community, and private sector.

DOD needs to develop an active layered cyber defense with offensive and defensive capabilities. Currently, most cyber defensive strategies rely on firewalls to block attacks. This method is similar to the post–World War I French creation of the Maginot Line,[8] which was an expensive defensive measure designed to keep the Germans out of France. But in 1940 the wall did not work. The Maginot Line was a single capability; the strategy of the line lacked both a layered defensive structure and the offensive capability needed for defense. To avoid a cyber Maginot Line, the United States needs layered, integrated defenses as well as an offensive capability.

Defining the Battlespace

The cyber domain has been created in a short time and has not had the same level of scrutiny as other battle domains. Land and sea domains have had thousands of years of discussion to create generally accepted definitions. The air domain has

Major Clifford S. Magee, USMC, is a Communications Officer currently serving with 13th Marine Expeditionary Unit and a 2012 graduate from the Marine Corps Command and Staff College.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **Awaiting Cyber 9/11**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Joint Force Quarterly ,260 Fifth Avenue, Building 64, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

had approximately 100 years of dedicated study. The discussions involving cyber as a battle domain are still nascent.

The rapid evolution and increasing complexity of the cyber domain have not allowed agreement even as to the definition of the cyber domain. Some define *cyberspace* as "the Internet," while the Central Intelligence Agency's (CIA's) statement to Congress is that "cyberspace is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography."[9] The official DOD definition of *cyber*—"a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers"[10]—is the most thorough definition but is so encompassing it is difficult to comprehend. Understanding the characteristics of cyberspace would assist in understanding the definition of the cyber domain.

Cyberspace is a manmade domain created by information technologies. It is composed of radio waves, cell phones, fiber optic cables, satellites, laser beams, software, firmware, and anything that can be linked together to create a network.[11] Some elements required to support cyberspace are electronic components, electricity, and an infrastructure to connect it all.

Understanding the characteristics of cyberspace supports an understanding of cyber warfare. Cyber warfare is generally divided into two core operational capabilities: computer network operations (CNO) and electromagnetic warfare (EW).

CNO is a broad term that encapsulates three subcategories:

- *Network defense* protects computers and networks.[12]
- *Network exploitation* gains information from other computer assets.[13]
- *Network attack* disrupts, denies, degrades, or destroys information or capability.[14]

In 2008, DOD suffered a major failure in its network defense.[15] It started when an infected flash drive was placed into a U.S. military laptop at a base in the Middle East.[16] An authorized user brought the flash drive into a facility, but the drive was infected with a virus created by a foreign intelligence agency. Once the user placed the flash drive into a computer, the malicious code spread throughout the DOD network undetected.[17] The virus infected both classified and unclassified networks[18] and silently gave control of DOD servers to unknown adversaries.[19] DOD has not released the full extent of the compromise, but the virus did have the ability to deliver information to adversaries clandestinely.[20] To clean and recover from what is described as the worst breach of U.S. military computers in history took 14 months and cost a billion dollars.[21]

Cyber espionage is a form of network exploitation that is currently a low-risk, high-gain activity. There are hundreds of exploitation programs and just one mid-range program globally exploits 50 times the

U.S. Air Force Academy cadets spend summer session in Cyber 256, Basic Cyber Operations course

U.S. Air Force (Raymond McCoy)

amount of data that was taken in the Wikileaks espionage case.[22] China, for example, has been accused of performing massive network exploitation operations against the U.S. Government and private industry. Attribution is difficult with network exploitation because even when perpetrators have been identified geographically, nations can claim that the exploitation was from a nongovernmental hacker acting independently. Whether state sponsored or not, Chinese hackers have been stealing intellectual research and development projects, software source code, and manufacturing know-how from the United States for years. The loss of intellectual property and government secrets due to network exploits has resulted in significant erosion of previous U.S. technological advantages.

A well-known form of network attack occurred in June 2010 when a computer virus named Stuxnet was discovered in powerplants and factories around the world.[23] More complex than any virus ever seen, Stuxnet was designed to attack industrial systems referred to as supervisory control and data acquisition (SCADA) systems. It had the ability to turn up the pressure inside nuclear reactors' centrifuge machines and switch off oil pipelines.[24] The virus exploited vulnerabilities that system creators were not aware of, referred to as "zero-day exploits."[25] Zero-day exploits are rare and extremely time-consuming to develop because they create vulnerabilities that have not been identified. Viruses rarely have even one zero-day exploit, but Stuxnet was so technologically advanced that it had four of these highly technical exploits.[26] Microsoft assessed that to create the virus took more than 10,000 man-hours.[27]

Stuxnet exploited vulnerabilities that system creators were not aware of, referred to as "zero-day exploits."

When Stuxnet was deployed, it was looking for a specific target; if it did not see its target, it would lie dormant. Stuxnet was a precision-guided munition designed to attack the centrifuges that spin nuclear material at Iran's enrichment facilities.[28] If this attack were a traditional kinetic attack, it would have been an act of war. However, since the definition of cyber warfare is unclear and cyber attacks are difficult to attribute, Iran did not declare war because it did not know who executed the attack. Intelligence experts report that 1,000 centrifuges in Iran's main enrichment facility in Nantanz had to be replaced after the attack,[29] delaying nuclear production capability by 2 years.

The weapon was relatively inexpensive to create, but Stuxnet is now a genie out of the bottle. The tremendously dangerous and sophisticated virus that successfully attacked a SCADA system is now available for free on the Internet, where one can find tutorials on how to design and even employ it. Therefore, it is a safe assumption that a variation of Stuxnet code will be reused to attack another institution in the near future.

Now that the technology of Stuxnet is widely available, it no longer requires a major financial investment or the backing of a nation-state. It can be copied and recreated easily. No fissile material or stealth technology is required, and it can be deployed at the speed of light. This demonstrates that the proliferation of cyber weapon technology cannot be easily controlled; the technology is cheap and spreading to traditional powers such as Russia and China as well as to terrorist organizations. Cyber weapon development is not going away; it will only proliferate.

The second operational capability in cyber warfare is electronic warfare. The DOD definition of *EW* is any military action that involves the use of the electromagnetic spectrum to include directed energy to control the electromagnetic spectrum to attack an enemy.[30] EW can be broken into three components: electronic attack, electronic protection, and EW support. The use of wireless Internet and cell networks has created a wide range of opportunities for the combination CNO and EW.

To protect government, industry, and national interests, the United States needs to adjust its current definition of the cyber world and develop doctrine for cyberwar. To quote Sun Tzu, "Invincibility lies in the defense; possibility of victory in the offense." In the cyber domain, the Nation remains primarily defense focused, but to ensure safety, it needs to advance its doctrine to include offensive cyber operations. Currently, U.S. adversaries do not fear negative consequences from their cyber operations. The possibility of painful cyber or kinetic retribution must be understood.

Cyber 9/11

Before the events of 9/11, terrorism was largely considered a criminal issue properly handled by law enforcement and the Intelligence Community.[31] Local police and the Federal Bureau of Investigation would arrest terror suspects, and the CIA was heavily engaged in intelligence collection against terrorist organizations. Terrorism was not a DOD focus. The events of 9/11 changed the focus for DOD, and the Defense Department now fills a major antiterror role because of the ferocity of the attacks.[32] Similar to 9/11, adversaries today will exploit the Nation's cyber defenses in an effort to destroy the American way of life.

Cyberwar has already begun. Its costs are low and its impacts can be great. The United States is the most target-rich country in the world, but military networks are not the prime targets—those are in the civilian sector. Former Secretary of Defense Leon Panetta warned, "the next Pearl Harbor will be a cyber attack."[33] Just as the attack on Pearl Harbor finally galvanized the U.S. Government and public sectors after years of aggressive Japanese actions throughout the Pacific, Secretary Panetta's warning is déjà vu. State and nonstate actors have been performing cyber operations against the United States at an alarming rate, and the loss of intellectual property as well as U.S. Government secrets has weakened the Nation's defense posture and negated its technological advantages. Yet it seems the "sleeping giant" is again awaiting a public, catastrophic event before awakening.

Defining critical infrastructure is a responsibility of Congress, but a series of Presidential decision directives defined *critical infrastructure* as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[34] This definition will need to be revised by Congress often as reliance on the cyber domain continues to grow.

In 2003, an engineering glitch in FirstEnergy, Incorporated, software caused a power outage throughout the Northeast and Midwest United States and parts of Canada, and 50,000,000 people lost power in 4 minutes.[35] This was not an attack. It was an inadvertent programming error.[36] However, if this had been an attack, the U.S. Government would not have had the ability or authorities to assist FirstEnergy. The United States lacks the ability for cyber coordination between government and private industry.

Placing DOD in charge of U.S. cyber defense would consolidate shared information about cyber attacks. A single point of information collection would create a cyber defense team approach between the private and public sectors. Attacks that occur in the private sector are rarely shared with the government. Even within the government, the .gov and .mil domains rarely share

Sailor uses hash analysis at Defense Cyber Investigations Training Academy

U.S. Air Force (Lance Cheung)

information on cyber attacks. Currently, DOD operates and protects the .mil domain, the Department of Homeland Security protects the .gov domain, and each private-sector entity is responsible for its own piece of the .com domain. There is no incentive for the private sector to reveal to the public sector the amount or types of cyber attacks that are occurring. Bank of America and most of the defense industrial base are not required to—and do not—reveal the types and numbers of attacks that are occurring within their systems. They, in fact, are disincentivized because customers, investors, and government entities contracting for their services may lose confidence in those companies' abilities to defend themselves.

Why DOD?

DOD has already created U.S. Cyber Command (USCYBERCOM), which is collocated in Fort Meade, Maryland, with the National Security Agency (NSA). This combination leveraged existing cyber capabilities that could not be replicated because the cost is prohibitive, and the intellectual resources resident at these institutions would be extremely difficult to recreate. Moreover, integration of USCYBERCOM and NSA provides the people, expertise, and equipment required to defend the United States in cyberspace. General Keith Alexander, USA, serves as commander of both USCYBERCOM and NSA, and he ensures that the partnership leverages the capabilities of both commands.

USCYBERCOM integrates the existing pool of personnel, has substantial funding, and is authorized to perform offensive cyber operations. It draws its personnel from the private sector, government, and Service components. NSA employs over 800 Ph.D.s and is the world's largest single employer of mathematicians.[37] The 24th Air Force, 10th Fleet (Navy), Marine Forces Cyber, and Army Forces Cyber provide personnel with expertise and experience in defending mission-critical networks.[38] The nuclear command and control Emergency Action Network is one of the 15,000 networks that DOD defends, making the Department the largest cyber network in the world.[39] DOD networks are located across hundreds of installations in dozens of countries around the globe. USCYBERCOM headquarters has a fiscal year 2012 budget of $159 million, and the DOD technology budget is approximately $38 billion.[40] USCYBERCOM thus provides the Nation an existing cyber defense capability, funding, and expertise that cannot be recreated or replicated.

USCYBERCOM has provided the .mil domain with the most capable cyber defense in the world, but the command is not authorized to direct the security of the .gov or .com domains. Legal authorities and response actions need to be authorized before a cyber attack is launched. Attacks against the United States would occur at "net-speed," and defenders of the U.S. cyber domain require maneuver space and authorities. If an attack against the .gov or .com domains occurs, it would not stop while the United States debates authorities.

The technical expertise required to view, understand, and coordinate actions in cyberspace is limited. General Alexander estimates that only about 1,000 people in the United States are currently qualified with the proper clearances, technical abilities, and certifications.[41] This small pool of trained and proficient "cyber warriors" is a high value commodity that is fought over between the public and private sectors. The current model of the private sector—which includes vital

U.S. Navy (Tom Jones)

Cyber systems operator with CJTF 435 awaits confirmation that network connections operate properly at Kabul University's Law and Political Science School

infrastructure and provides its own defense without government assistance—does not leverage the limited workforce that exists in cyber defense. Designating DOD as the lead for cyber defense would leverage the small pool of experts and assist in cyber collaboration.

Cyber COP

To protect financial systems, power grids, telecommunications, water supplies, intellectual property, and military communications, the United States must generate a comprehensive picture of cyberspace. A cyberspace common operational picture (COP) that fuses the public and private realms would provide the Nation a tool that could be used to prevent, detect, and recover from attacks. DOD needs to be provided the command structure, resources, and authorities to monitor, enact, and enforce security standards on the Internet. This is a national security issue because it affects the U.S. economy and defense.

To defend cyberspace, the United States needs to develop its situational awareness of the cyber domain. The U.S. Government and private sector are connected to the same commercial infrastructure. The cyber COP needs the ability to merge government and private-sector cyber pictures to focus efforts on known and emerging threats and to provide U.S. "cyber warriors" with the ability to outmaneuver adversaries in the defense or on the attack.

The proposed cyber COP can be understood by dividing it into blue, red, and white feeds. *Blue feeds* represent friendly devices that support our cyber networks.[42] *Red feeds* represent threats to the network to include adversaries, physical damage, accidents, and equipment failures.[43] *White feeds* provide situational awareness of activities outside of the U.S. cyber domain, focusing on emerging threats to provide defenders a proactive intelligence capability.[44]

When the Armed Forces select a position in the real world, the focus is on selecting, capturing, and retaining key terrain. Similarly, the cyber COP would focus on key *cyber* terrain. The cyber terrain would need to be a prioritized list of key nodes that encompass the .gov, .mil, and .com domains. Visibility of the key cyber terrain would assist in situational awareness of cyberspace. Situational awareness is vital for timely and effective cyber responses. Situational awareness of the land, sea, air, and space domains would also be vital. For example, a relatively simple Global Positioning System denial of service in response to an attack could have dramatic unforeseen impacts on the commercial sector (for example, shipping or aviation) or precision fires for the military.

In the past, DOD has relied on units moving into position as an indication or warning that an attack could occur. Learning of an imminent attack when forces are already in place is too late; combatant commanders need more time to prepare effective responses. Future conflicts will be preceded by an increased amount of cyber activity. An example is the 2008 Russian invasion of Georgia that successfully coordinated cyber attacks with kinetic attacks. The cyber COP would be able to sense traffic for anomalies that could provide indications or warnings that could push combatant commanders' timelines to the left.

The cyber COP would also assist in offensive cyber operations. Recent attacks on U.S. corporations such as Google, the Nasdaq stock exchange, Lockheed Martin, Symantec, and many others have demonstrated the threat to the private sector. After a lengthy forensic process, some of the attacks were attributed to China and Russia. These attacks occur daily and the attackers do not fear cyber retaliation. Retaliatory cyber tools exist—a cyber tool was recently developed by Japanese defense engineers,[45] a digital virus that can track down, identify, and disable attacking systems. The United States needs to assist in the defense of key private-sector industries by providing an offensive capability.

cyber security is a team sport that requires players from the private and public sectors to share information

The framework for prioritization of fused information from the .mil, .com, and .gov domains has been developed and is currently operational in DOD, which focuses on categorizing vulnerabilities, threat activities, and their most likely consequences. The threat category and the severity of the threat drive resources, time, and attention given to an identified problem. The fused cyber COP would alert DOD of a threat to U.S. national interests.

Regulation Reform Required

To protect the American people, the U.S. Government has placed many types of regulations over the nuclear, electrical, health care, financial, and defense industries as well as government institutions, but has not created any meaningful regulations on cyber security. The government has a responsibility to ensure that it and private companies of vital national interest are compliant with current best practices of cyber security policies. It also needs to set and regulate standards with respect to encryption and data protection as well as task DOD with ensuring cyber security compliance.

Cyber security is currently in its Wild West era where anything goes. There are no baseline requirements for cyber security, and companies are free to decide for themselves what constitutes enough security. Yet 73 percent of American Internet users have been victims of cyber crimes. According to MacAfee, the cost of cyber crimes globally has passed $1 trillion because of lost intellectual property and damaged equipment.[46] DOD reports that its networks are probed for weaknesses about 250,000 times an hour.[47] The growth of and increased threat against e-commerce alone has made cyber security essential for national defense.

The government has a responsibility to set regulations and ensure compliance of cyber security. DOD, with collaboration from DHS, the Intelligence Community, and private sector, needs to publish required baseline settings for firewalls, antivirus software, and encryption systems. Regulated and assured compliance of cyber security practices in key industries is a requirement for national security.

Conclusion

Today, the only entity not in the .com and .gov domains is DOD.[48] China, Russia, terrorist organizations, criminal gangs, teenage hackers, and anarchists have already paved roads into these domains, as well as into the .mil domain. The United States needs to develop a cyber strategy that protects government and extends protection to the Nation's privately owned critical infrastructure. Cyber security is a team sport that requires players from the private and public sectors to share information about vulnerabilities. The aggregated information would improve situational awareness and be the basis for a cyber COP. Improved collaboration would also be mutually beneficial for the private and public sectors.

DOD should be given the authority to lead the United States in cyber defense. An amendment to United States Code, Title 10, Armed Forces, to allow DOD to perform cyber investigations would leverage its intellectual capital, technical expertise, equipment, and funding, which cannot be recreated or replicated; therefore, selecting DOD would be an efficient use of the Nation's resources. DOD already has some authorities to offensively respond to protect the United States in the cyber domain. State and non-state actors currently penetrate and exploit American cyberspace with no fear of retaliatory strikes. DOD is prepared and could provide a near real-time offensive response to cyber warfare.

The current model of networking in the United States is indefensible; DOD alone has 7 million devices working off of 15,000 disparate networks managed independently.[49] Recent technological innovations such as "cloud computing" must be leveraged to create a more secure, reliable, and cost-effective cyberspace. For example, collapsing the 15,000 disparate DOD networks to a cloud environment would provide it the ability to react to threats at "net-speed." This model must be used and coordinated with critical public and private sectors.

Vulnerability in the cyber domain threatens the security and prosperity of the Nation. Currently, the United States does not have an organization that has the capabilities or authorities to oversee cyber security for the public and private sectors. To defend against the ever-increasing number and complexity of cyber attacks, the U.S. Government needs to identify the Department of Defense as lead in cyber defense and enhance its authorities to fill that role. **JFQ**

NOTES

[1] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, prepared for the U.S.-China Economic and Security Review Commission (McLean, VA: Northrop Grumman, 2009), 41.

[2] Ibid., 42.

[3] Richard Clarke, "China's Cyberassault on America," *The Wall Street Journal*, June 15, 2011, available at <http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html>.

[4] Krekel, 43.

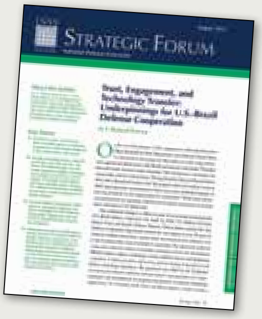
[5] Clarke.

[6] Lieutenant Colonel David Fahrenkrug, chief strategist for 8th Air Force, interview by Harold Channer, April 17, 2008.

[7] Fahrenkrug, interview.

[8] General Keith B. Alexander, USA, commander, U.S. Cyber Command, interview by Peter Alphonso, May 3, 2011.

[9] B.G. Kutais, *Internet Policies and Issues* (Hauppauge, NY: Nova Science Publishers, 2002), 2.



[10] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, 2009), I-7.

[11] Fahrenkrug, interview.

[12] Government Accountablility Office (GAO), *Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates*, GAO-11-695R (Washington, DC: GAO, July 29, 2011), 2.

[13] Ibid.

[14] Ibid.

[15] William J. Lynn III, speech, "Defending a New Domain: Cyber Security," Washington, DC, 2010.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Eric Chambrow. *Gov Info Security,* November 8, 2011, available at <www.govinfosecurity.com/blogs.php?postID=1115>.

[21] Alexander, interview.

[22] Krekel, 57.

[23] Ryan Naraine, "Stuxnet attackers used 4 Windows zero-day exploits," *ZD Net.com*, September 14, 2010, available at <www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347>.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Michael Bame, *About.com*, December 6, 2010, available at <http://defense.about.com/b/2010/12/06/stuxnet-virus-targets-iran-cyber-warfare.htm>.

[28] Ibid.

[29] Atika Shubert, "Cyber warfare: A different way to attack Iran's reactors, *CNN.com*, November 8, 2011, available at <http://articles.cnn.com/2011-11-08/tech/tech_iran-stuxnet_1_stuxnet-centrifuges-natanz-facility?_s=PM:TECH>.

[30] JP 3-13.1, *Electronic Warfare* (Washington, DC: The Joint Staff, 2007), v.

[31] Robert B. Bruce, interview by Cliff Magee, February 8, 2012.

[32] Ibid.

[33] Lisa Daniel, "Panetta: Intelligence Community Needs to Predict Uprisings," American Forces Press Service, February 11, 2011.

[34] Michael V. Hayden, "Black Hat USA 2010: Cyber war: Are we at war? And if we are, how should we fight it?" *YouTube.com*, available at <www.youtube.com/watch?v=XXnIvBBASLI&feature=relate>.

[35] Michael F. Hordeski, *Megatrends for Energy Efficiency and Renewable Energy* (Lilburn, GA: Fairmont Press, 2011), 238.

[36] Ibid.

[37] Alexander, interview.

[38] Ibid.

[39] Ibid.

[40] Teresa Takai, "The DoD Information Enterprise," *Chips Magazine*, October–December 2011.

[41] Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security," *NPR.org*, July 19, 2010, available at <www.npr.org/templates/story/story.php?storyId=128574055>.

[42] Brigadier General John A. Davis, USA, director of Current Operations, U.S. Cyber Command, interview by the Armed Forces Communications and Electronics Association, February 2011.

[43] Ibid.

[44] Ibid.

[45] George V. Hulme, "Government engineers actively plan for cyberwar," *CSO Online.com*, January 4, 2012, available at <www.csoonline.com/article/697365/government-engineers-actively-plan-for-cyberwar>.

[46] Alexander, interview.

[47] Ibid.

[48] Ibid.

[49] Hayden.